ارزیابی امنیتی سه پروتکل احرازهویت مبتنی بر PUF مناسب شبکه پهپادها به روش صوری و با استفاده از ابزار تحلیل خودکار ProVerif و مقایسه سرعت محاسباتی آنها

سیدهادی نورانی اصل [۱] و جواد علیزاده [۲]

۱- دانشجوی کارشناسی ارشد مخابرات امن، مرکز علم و فناوری فتح، دانشگاه جامع امام حسین(ع)، تهران، ایران

۲- استادیار، مرکز علم و فناوری فتح، دانشگاه جامع امام حسین(ع)، تهران، ایران

چکیده

مفهوم اینترنت اشیا، یک فناوری متحول کننده هست که از پیشرفت‌های اخیر در حوزه شبکه‌های کامپیوتری و اینترنت حاصل شده است. به عنوان یک مصداق مهم از این مفهوم می‌توان به استفاده از پرنده‌های هدایت‌پذیر از دور یا پهپادها اشاره کرد که کاربردهای زیادی در حوزه‌های کشاورزی، هوانوردی، نظارت‌های هوایی و نظامی دارند. برای استفاده مناسب از پهپادها لازم است اطمینان حاصل شود که افراد غیر مجاز به اطلاعات ارسالی پهپادها دسترسی نداشته و نتوانند یک پهپاد مجاز را جعل کنند. برای این منظور در شروع ارتباطات پهپادها از پروتکل‌های احراز هویت استفاده می‌شود که در سال‌های اخیر توجه زیادی به طراحی و تحلیل و ارزیابی آنها شده است. از این پروتکل‌ها می‌توان SecAuthUAV، Drone-MAP و PMAP را نام برد که در سال‌های ۲۰۲۰ تا ۲۰۲۲ طراحی شده‌اند. طراحان پروتکل‌ها برای ارزیابی امنیت طرح‌های خود بیشتر از روش‌های غیرصوری استفاده کردند حال آنکه برای اطمینان از امنیت این پروتکل‌ها، لازم است تا در کنار روش‌های غیرصوری، از روش‌های صوری و ابزارهای تحلیل خودکار مبتنی بر این روش‌ها نیز استفاده شود. در این مقاله سه پروتکل ذکر شده که جزو پروتکل‌های احراز اصالت مبتنی بر توابع کپی‌ناپذیر فیزیکی (PUF) هستند، با استفاده از ابزار تحلیل خودکار ProVerif، یک ابزار ارزیابی مبتنی بر روش صوری، تحلیل می‌شوند. خروجی تحلیل‌ها نشان می‌دهد که از نگاه صوری، این پروتکل‌ها ضعف امنیتی ندارند. در این مقاله همچنین پروتکل‌های مورد نظر با توجه به عملیات محاسباتی که در آنها به کار رفته است، از لحاظ سرعت محاسباتی با هم مقایسه شده‌اند که با توجه به نتایج کار، پروتکل Drone-MAP نسبت به دو پروتکل دیگر از سرعت محاسباتی بالایی برخوردار است.

کلمات کلیدی: امنیت پهپاد، احراز هویت، تحلیل صوری، ابزار ProVerif

۱. مقدمه

در حال حاضر اهمیت کاربرد شبکه‌های کامپیوتری در جنبه‌های مختلف زندگی انسان بر کسی پوشیده نیست. پیشرفت‌ها در حوزه شبکه‌های کامپیوتری مانند اینترنت، شبکه‌های بی‌سیم و ابزارهای ارتباطی سیار باعث ایجاد تغییرات قابل توجهی در شیوه زندگی بشر شده است. مفهوم اینترنت اشیاء [۲] (IoT) یک دستاورد متحول کننده است که از پیشرفت‌های مذکور حاصل شده و کاربردهای بسیاری در حوزه‌های مختلف مانند سلامت پزشکی، کشاورزی و نظامی پیدا کرده است [۱]. به عنوان یک مصداق از مفهوم IoT می‌توان به کنترل و استفاده از وسایل نقلیه هوایی بدون سرنشین [۳] (UAV) یا پهپادها اشاره کرد [۲]. این فناوری کاربرد زیادی در حوزه نظامی دارد ولی با این وجود نباید از تاثیرات مثبت آن در حوزه‌های

[1] Email: hadinorani@ihu.ac.ir
[2] Internet of Things
[3] Unmanned aerial vehicles

کشاورزی، هوانوردی، نظارت‌های هوایی و غیره غافل شد. واژه اینترنت پهپادها[1] (IoD) که در منابع علمی آورده می‌شود را می‌توان به طور خلاصه به معنی کاربرد IoT در حوزه پهپادها در نظر گرفت.

نفوذ IoT در زندگی بشر، فواید غیرقابل انکاری دارد. اما باید توجه داشت که این امر منجر به چالش‌ها، تهدیدات و آسیب‌پذیری‌های متنوعی مانند نقض حریم خصوصی کاربران، جعل هویت و استفاده غیرمجاز از اطلاعات ایشان شده است [۳]. در مورد یک پهپاد این مسائل می‌تواند منجر به از کار افتادن پهپاد، ارسال اطلاعات نادرست توسط آن، ربوده شدن و کشف اطلاعات محرمانه پهپاد شود. برای جلوگیری از این آسیب‌پذیری‌ها لازم است امنیت اطلاعات و ارتباطات در پهپادها تامین شود. در برخی موارد به جای یک پهپاد، شبکه‌ای از پهپادها استفاده می‌شود که در اینجا نیز می‌بایست الزامات امنیتی مانند احراز هویت پهپادها در تقابل با یکدیگر یا احراز هویت یک پهپاد توسط سامانه کنترل کننده و برعکس، برآورده شوند. در سال‌های اخیر، پروتکل‌های احراز اصالت متنوعی برای تامین امنیت شبکه پهپادها معرفی شده است که از جمله آنها می‌توان به [۴-۶] اشاره کرد. همراه با توسعه و پیشرفت دانش طراحان، تحلیلگران و مهاجمان نیز دانش خود را توسعه دادند و توانستند حملات جدیدی روی پروتکل‌های جدید ارائه دهند [۷-۹]. برای اطمینان خاطر از امنیت یک پروتکل احراز اصالت لازم است تا این پروتکل هم به روش غیرصوری[2] و هم به روش صوری[3] مورد تحلیل و ارزیابی قرار گیرد. منظور از تحلیل به روش غیرصوری، بررسی مقاومت پروتکل در برابر حملات شناخته شده مانند حمله انکار سرویس[4]، حمله مردی در میانه[5]، حمله جعل[6] و غیره است. در تحلیل به روش صوری نیز یک صور و ظاهر از پروتکل در نظر گرفته می‌شود و با استفاده از روش‌های مبتنی بر منطق و روابط ریاضیاتی بررسی می‌شود که یک پروتکل نشت اطلاعات محرمانه نداشته باشد. روش‌های صوری که در مقالات مختلف برای ارزیابی پروتکل‌ها استفاده می‌شود در دو دسته روش‌های مبتنی بر منطق مانند منطق BAN [۱۰] و منطق Mao Boyd [۱۱] و همچنین تحلیل با استفاده از ابزارهای خودکار مانند ProVerif [۱۲]، Scyther [۱۳]و Avispa [۱۳] قابل ذکر هستند. از میان روش‌های صوری، روش‌های تحلیل خودکار به دلیل سرعت و دقت بالا از اهمیت بیشتری برخوردار می‌باشند. لازم به ذکر است از آنجا که ابزارهای تحلیل خودکار متنوع هستند، اگر برای بررسی امنیت یک پروتکل از ابزارهای متنوع استفاده شود، اطمینان خاطر بیشتری حاصل می‌شود که این طرح نشت اطلاعات محرمانه نداشته باشد.

در سال ۲۰۲۰، علادی[7] و همکاران [۱۴] یک پروتکل احراز اصالت به نام SecAuthUAV که مبتنی بر توابع کپی‌ناپذیر فیزیکی[8] (PUF) است را پیشنهاد کردند. در این پروتکل نیازی به ذخیره مقادیر محرمانه در پهپادها نیست و علاوه بر ارتباط میان یک پهپاد و ایستگاه زمینی، ارتباطات میان دو پهپاد نیز پشتیبانی می‌شود. در فرآیند احراز هویت پهپاد با ایستگاه زمینی، یک کلید جلسه امن بین آنها به اشتراک گذاشته می‌شود که برای این کار از PUF تعبیه شده در پهپادها استفاده می‌شود. پروتکل SecAuthUAV ویژگی‌های امنیتی مانند احراز هویت متقابل، ناشناس بودن پهپاد و محرمانگی رو به جلو را تضمین می‌کند. طراحان برای ارزیابی امنیتی طرح خود از روش‌های غیرصوری استفاده کرده و نشان دادند که این طرح در برابر حملات شناخته شده مانند حمله جعل و حمله مردی در میانه مقاوم هست. آنها همچنین از منطق Mao Boyd [۱۱] نیز برای ارزیابی امنیتی طرح خود استفاده کردند و با توجه به نتایج کار ادعا کردند پروتکل SecAuthUAV امنیت اثبات‌پذیر دارد. با این وجود در ارزیابی امنیتی این پروتکل از ابزارهای تحلیل خودکار استفاده نشده است. حال آنکه

[1] **Internet of drone**
[2] **Non-formal**
[3] **Formal**
[4] **Denial of Service**
[5] **Man in the middle.**
[6] **Counterfeiting**
[7] **Alladi**
[8] **Physical Unclonable Functions**

برای اطمینان بیشتر در مورد امنیت این طرح لازم هست تا نتایج تحلیل با استفاده از یک یا چند ابزار تحلیل خودکار نیز مطالعه شود. در یک کار دیگر در سال ۲۰۲۱ علادی و همکاران [۱۵]، پروتکل احراز اصالت دیگری به نام Drone-MAP ارائه کردند که مشابه SecAuthUAV مبتنی بر PUF طراحی شده است. در مقایسه اول دو پروتکل Drone-MAP و SecAuthUAV، می‌توان گفت که پروتکل اخیر نیز ویژگیهایی مانند احرازهویت متقابل، محرمانگی و امنیت دربرابر دستکاری فیزیکی را تامین می‌کند. همچنین ارزیابی امنیتی آن نیز با استفاده از روش‌های غیر صوری انجام شده است؛ اما از روش‌های مبتنی بر ابزارهای خودکار در تحلیل آن استفاده نشده است. در سال ۲۰۲۲ کانگ‌پو[1] و همکاران [۴] یک پروتکل احراز اصالت به نام PMAP برای شبکه پهپادها ارائه کردند که مشابه دو پروتکل قبلی مبتنی بر PUF می‌باشد. این پروتکل ویژگی‌های احرازهویت متقابل و امنیت در برابر دستکاری فیزیکی را تامین می‌کند. برای تحلیل و ارزیابی این پروتکل از روش‌های غیرصوری استفاده شده است. همچنین از ابزار تحلیل خودکار Avispa نیز برای تحلیل صوری این طرح استفاده شده است که نشان می‌دهد پروتکل PMAP نشت اطلاعات محرمانه ندارد.

در این مقاله دو طرح SecAuthUAV و Drone-MAP که در تحلیل و ارزیابی آنها از روش‌های تحلیل خودکار استفاده نشده است، با استفاده از ابزار ProVerif که یک ابزار رایج برای تحلیل صوری پروتکل‌ها است، از نگاه صوری مورد ارزیابی قرار می‌گیرند تا نتایج این تحلیل در کنار تحلیل‌های قبلی که طراحان از طرح خود داشتند، باعث جمع‌بندی دقیق‌تر از امنیت این طرح‌ها شود. علاوه بر این، پروتکل PMAP که بر خلاف دو پروتکل قبلی با ابزار تحلیل خودکار Avispa مورد ارزیابی قرار گرفته بود، یک بار دیگر با ابزار ProVerif مورد تحلیل و ارزیابی قرار می‌گیرد تا اطمینانی در جهت تایید خروجی‌های تحلیل با Avispa یا نتایج تحلیل‌های دیگر حاصل شود. در بخش دیگر این مقاله، سه طرح SecAuthUAV، Drone-MAP و PMAP از نظر کارآیی محاسباتی و عملگرهایی که در آنها به کار گرفته شدند، مورد مطالعه و بررسی قرار می‌گیرند و سرعت محاسباتی آنها باهم مقایسه می‌شوند. برای پوشش اهداف ذکر شده، مطالب مقاله به این صورت سازماندهی شده است که در بخش دو، سه پروتکل احراز هویت مبتنی بر PUF توصیف می‌شوند. در بخش سه که بخش اصلی این مقاله هست، این پروتکل‌ها با زبان ProVerif پیاده‌سازی شده و مورد ارزیابی صوری قرار می‌گیرند. در بخش چهار، با مقایسه سرعت محاسباتی این پروتکل‌ها به این سوال پاسخ داده می‌شود که از بین سه طرح بررسی شده در این مقاله کدام طرح سرعت محاسباتی بالایی دارد. در نهایت جمع‌بندی و نتیجه‌گیری مقاله در بخش پنج ارائه می‌شود.

۲. پروتکل‌های احراز هویت مبتنی بر PUF در شبکه پهپادها

در سال‌های اخیر پروتکل‌هایی که برای تامین امنیت در شبکه پهپادها ارائه شده‌اند از ویژگی‌های توابع کپی‌ناپذیر فیزیکی (PUF) استفاده می‌کنند تا باعث افزایش مقاومت در برابر حملاتی مانند حملات مربوط به در اختیار گرفتن پهپاد شوند [۱۶-۱۸]. عملکرد یک PUF مبتنی بر فرآیند چالش و پاسخ است. یعنی PUF دارای خاصیتی است که وقتی یک محرک ورودی به نام چالش به آن وارد شود، یک پاسخ منحصر به فرد برای چالش تولید می‌کند. انتظار می‌رود دو دستگاه PUF مختلف، پاسخ‌های متفاوتی را با توجه به چالش‌های مشابه ایجاد کنند. به عبارت دیگر تراشه PUF تعبیه شده به عنوان یک اثر انگشت منحصر به فرد و غیر قابل کپی برای هر پهپاد در شبکه عمل می‌کند. یک تابع PUF با استفاده از رابطه ریاضی به شکل زیر قابل بیان است که در آن منظور از C و R به ترتیب چالش و پاسخ می‌باشد.

$$\mathbf{R = PUF(C)}$$

در ادامه این بخش پروتکل‌های SecAuthUAV، Drone-MAP و PMAP توصیف می‌شوند. برای این کار از نمادگذاری معرفی شده در جدول ۱ استفاده شده است.

[1] **Cong Pu**

جدول ۱: نمادهای استفاده‌شده

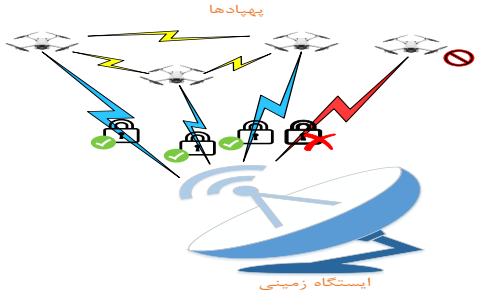
نمادها	توضیحات
U_i	پهپاد
$\mathbf{ID_i}$	شناسه پهپاد
UID_i	شناسه موقت پهپاد
GS	ایستگاه زمینی
GID	شناسه ایستگاه زمینی
$\mathbf{puf}$	توابع کپی‌ناپذیر فیزیکی
$\|\|$	الحاق
$\oplus$	عملگر XOR
$(M)_K$	پیام M با کلید K رمزگذاری شده است
$H()$	تابع چکیده‌ساز
$MAC()$	کد احراز هویت پیام
SK_i	کلید نشست
$\mathbf{N_X}$	عدد تصادفی
$F()$	تابع غیر خطی عمومی با ورودی و خروجی ۳۲ بیتی
$(\mathbf{C}, \mathbf{R})$	زوج چالش و پاسخ
$K_1, K_2, \ldots, K_M$	زیرکلیدها

توصیف پروتکل احراز هویت SecAuthUAV

در سال ۲۰۲۰ علادی و همکاران یک طرح برای احراز هویت پهپاد با ایستگاه زمینی و پهپاد به پهپاد ارائه کردند [۱۴]. این پروتکل شامل بخش معماری، تبت‌نام پهپاد، فرآیند احرازهویت پهپاد با ایستگاه زمینی و احراز هویت پهپاد با پهپاد می‌باشد. در این بخش این پروتکل به صورت مختصر معرفی می‌شود. از آنجا که هسته اصلی امنیت در پروتکل مربوط به بخش احراز هویت پهپاد با ایستگاه زمینی است، بنابراین روی معرفی و تحلیل و ارزیابی صوری این بخش تمرکز خواهد شد.

مدل شبکه‌ای استفاده شده در پروتکل SecAuthUAV

مدل شبکه معرفی شده برای پروتکل SecAuthUAV، شامل پهپادها و یک ایستگاه زمینی است که در شکل ۱ نشان داده شده است. پهپادها دارای حافظه و قابلیت محاسباتی محدودی در مقایسه با ایستگاه زمینی هستند. در این مدل، چندین پهپاد ممکن است به یک ایستگاه زمینی متصل شوند. هدف این طرح ایجاد یک جلسه ارتباطی امن بین پهپادها وهمچنین پهپاد با ایستگاه زمینی با احراز هویت متقابل بین آنها است.



شکل ۱: مدل شبکه پروتکل SecAuthUAV

فرآیند احرازهویت پهپاد با ایستگاه زمینی

نحوه احراز هویت متقابل میان یک پهپاد و ایستگاه زمینی با استفاده از نمادگذاری معرفی شده در جدول ۱، مطابق شکل ۲ قابل بیان است. با توجه به این شکل بعد از انجام برخی محاسبات در طرف پهپاد و ایستگاه زمینی و تبادل چند پیام در نهایت احراز هویت میان پهپاد و ایستگاه زمینی صورت گرفته و برای ارتباطات امن بعدی یک کلید نشست به اشتراک گذاشته می‌شود. از این کلید نشست برای احراز هویت متقابل دو پهپاد هم کمک گرفته می‌شود که در این مقاله این بخش توضیح داده نشده است و برای دریافت جزییات بیشتر می‌توان به مقاله پروتکل SecAuthUAV مراجعه کرد.

پهپاد	ایستگاه زمینی
$generate\ \mathrm{N_A}$ $\mathrm{R} = \mathrm{PUF(C)}$ $h1 = H(R \parallel UID_i \parallel N_A)$ $UID_i, N_A, h1$ ⟹	چک کردن ثبت‌نام پهپاد پهپاد از دیتابیس (C, R) **بازیابی** $verify\ h1$ **تبدیل** R **به** K_1, K_2 N_B $X_1 = N_A \oplus K_2$ $Y_2 = N_B \oplus X_1 \oplus K_1$ $Q = (Y_2 \parallel X_1) \oplus (K_2 \parallel K_1)$ $h2 = H(Q \parallel GID \parallel N_B \parallel N_A)$ ⟸ $Q, h2$
تبدیل R **به** K_1, K_2 $Y_2 \parallel X_1 = K_2 \parallel K_1 \oplus \mathrm{Q}$ $N_B = Y_2 \oplus X_1 \oplus K_1$ $N_A = X_1 \oplus K_2$ $Verify\ h2$ N_C **استفاده از** N_C **برای تولید** (C', R') **از** puf $M' = R' \oplus K_2 \parallel K_1$ $N' = N_C \oplus K_1$ $(SK_i) = (K_1 \oplus N_B) \parallel (K_2 \oplus N_C)$ $h3 = H(R' \parallel UID_i \parallel N_B \parallel N_C \parallel SK_i)$ $M', N', h3$ ⟹	$N_C = N' \oplus K_1$ $R' = M' \oplus K_2 \parallel K_1$ $(SK_i) = (K_1 \oplus N_B) \parallel (K_2 \oplus N_C)$ $Verify\ h3$ ذخیره $(\mathrm{C}', \mathrm{R}')$
$\mathrm{UID'_i} = \mathrm{H(K_2 \| UID_i \| K_1)}$	$\mathrm{UID'_i} = \mathrm{H(K_2 \| UID_i \| K_1)}$

شکل۲: فرآیند احراز هویت و توافق کلید نشست میان پهپاد و ایستگاه زمینی در پروتکل SecAuthUAV

توصیف پروتکل احرازهویت Drone-MAP

در سال ۲۰۲۱ علادی و همکاران [۱۵] پروتکل احراز هویت برای شبکه پهپادها به نام Drone-MAP ارائه کردند. معماری شبکه‌ای این طرح و مراحل ثبت‌نام و احراز هویت پهپاد با پهپاد مشابه پروتکل SecAuthUAV است که در بخش قبل معرفی شد.

فرآیند احرازهویت پهپاد با ایستگاه زمینی

فرآیند احراز هویت یک پهپاد با ایستگاه زمینی با استفاده از پروتکل Drone-MAP مطابق نمادگذاری جدول ۱، در شکل ۳ ارائه شده است. مطابق این شکل هنگامی‌که یک پهپاد با شناسه $\mathrm{ID_i}$ می‌خواهد یک ایستگاه زمینی نزدیک با شناسه GID را احراز هویت کند یا هویت خود را برای ایستگاه زمینی احراز نماید، $\mathrm{ID_i}$ و نانس $\mathrm{N_A}$ را به ایستگاه زمینی می‌فرستد. ایستگاه زمینی در حافظه خود بررسی می‌کند که آیا $\mathrm{ID_i}$ قبلاً در مرحله ثبت نام، ثبت شده است یا خیر. همچنین تازه بودن نانس نیز بررسی می‌شود. اگر هر یک از شرایط ناموفق باشد، درخواست احراز هویت توسط پهپاد خاتمه می‌یابد. در غیر این صورت محاسبات مطابق شکل ۳ انجام می‌شود تا در نهایت نتیجه عمل احراز هویت مشخص شود. کلیدهای $K_1, K_2, \dots, K_M$ از پاسخ R و با استفاده از روش ارائه شده در [۱۹] تولید می‌شوند.

پهپاد	ایستگاه زمینی
$generate\ N_A$	
$N_A, \mathrm{ID_i} \Longrightarrow$	
	$generate\ N_B$
	از دیتابیس (C, R) پیدا کردن
	$Q = (Y_m \| X_{m-1}) \oplus (K_m \| K_{m-1})$
	$N = m \oplus K_{m+1}$
	$h1 = H(GID \| Q \| m \| N_A \| N_B)$
	$\Longleftarrow C, Q, N, h1$
$R = PUF(C)$	
$m = N \oplus K_{m+1}$	
$(Y_m \| X_{m-1}) = Q \oplus (K_m \| K_{m-1})$	
$Verify\ h1$	
$new\ (C', R')$	
$R' = PUF(C')$	
$generate\ N_C$	
$M' = C' \oplus K_{m+2}$	
$M'' = R' \oplus K_{m+3}$	
$N' = N_C \oplus K_{m+4}$	
$S_k = F(K_{m+5} \oplus N_B) \oplus F(K_{m+6} \oplus N_C)$	
$h2 = H(U_{ID} \| R' \| m \| N_C \| S_k)$	
$M', M'', N', h2 \Longrightarrow$	
	$C' = M' \oplus K_{m+2}$
	$R' = M'' \oplus K_{m+3}$
	$N_C = N' \oplus K_{m+4}$
	$S_k = F(K_{m+5} \oplus N_B) \oplus F(K_{m+6} \oplus N_C)$
$\mathrm{ID'_i} = H(\mathrm{ID_i} \| K_{m+7})$	$\mathrm{ID'_i} = H(\mathrm{ID_i} \| K_{m+7})$

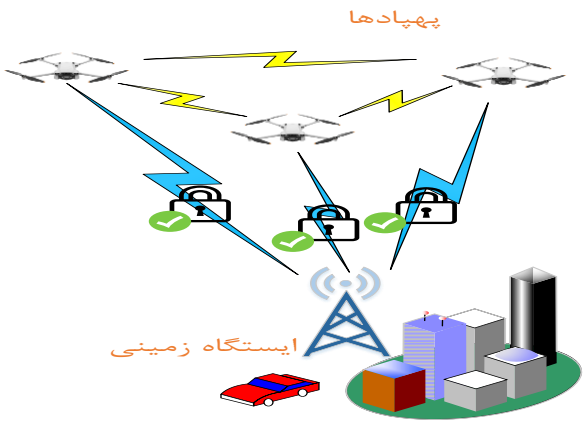
شکل۳: فرآیند احراز هویت و توافق کلید نشست میان پهپاد و ایستگاه زمینی در پروتکل Drone-MAP

توصیف پروتکل احرازهویت PMAP

در سال ۲۰۲۲ کانگ‌پو و همکاران [۴] پروتکل احراز هویت و توافق کلید همزمان سبک‌وزن PMAP برای شبکه پهپادها ارائه و روی ویژگی حفظ حریم خصوصی این پروتکل تاکید کردند. این پروتکل نیز همانند دو طرح قبل از یک PUF برای پشتیبانی از احراز هویت متقابل و ایجاد یک کلید جلسه امن استفاده می‌کند.

مدل شبکه‌ای استفاده شده در پروتکل PMAP

مدل شبکه‌ای پروتکل PMAP در شکل ۴ آورده شده است. در این مدل دو نهاد ارتباطی پهپاد و ایستگاه زمینی وجود دارد و دو حالت احراز اصالت میان پهپاد با ایستگاه زمینی و پهپاد با پهپاد در نظر گرفته می‌شود. فرض می‌شود هر پهپاد مجهز به یک PUF است. ایستگاه زمینی به عنوان یک موجودیت قابل اعتماد در نظر گرفته می‌شود و محدودیتی در منابع ندارد. بااین‌حال، پهپادها قابل اعتماد نیستند و منابع محدودی دارند. ارتباط بین موجودیت‌ها از طریق یک کانال بی‌سیم ناامن رخ می‌دهد و بنابراین باید امنیت این ارتباط تامین شود.



شکل ۴: مدل شبکه پروتکل PMAP

فرآیند احرازهویت پهپاد با ایستگاه زمینی

توضیحات مربوط به فرآیند احراز هویت پهپاد با ایستگاه زمینی در پروتکل PMAP به طور خلاصه در شکل ۵ ارائه شده است. با توجه به این شکل پهپاد و ایستگاه زمینی ابتدا یک پیام رمزگذاری شده را مبادله می‌کنند که از طریق مقدار تصادفی توسط پهپاد ایجاد می‌شود. همچنین آنها از زوج چالش و پاسخ برای تأیید هویت یکدیگر کمک می‌گیرند. اگر تأیید موفقیت‌آمیز باشد، پهپاد و ایستگاه زمینی به تبادل دو پیام رمزگذاری شده برای به اشتراک گذاشتن دو عدد تصادفی منحصر به فرد اقدام می‌کنند. درنهایت، پهپاد و ایستگاه زمینی از این دو عدد تصادفی منحصر به فرد برای محاسبه نام مستعار جدید و زوج چالش و پاسخ پهپاد استفاده می‌کنند و یک کلید جلسه امن ایجاد می‌کنند.

ایستگاه زمینی	پهپاد
	$\mathrm{UID}_i^t = \mathrm{H}(\mathrm{ID}_i \parallel \mathrm{R}_i^t)$ $generate\ \mathrm{N}_i^t$ $\mathrm{M}_1 = \mathrm{S}(\mathrm{UID}_i^t \parallel \mathrm{GID} \parallel \mathrm{N}_i^t)_{(\mathrm{C}_i^t, \mathrm{R}_i^t)}.$ $MAC_1 = C(M_1 \parallel \mathrm{N}_i^t)$ $\mathrm{M}_1, \mathrm{MAC}_1 \Rightarrow$

بازیابی UID_i^t و N_i^t از M_1 $MAC_1' = C(M_1 \parallel N_i^t)$ $MAC_1' =^? MAC_1$ $generate\ N_s^{t+1}$ $M_2 = S\left(UID_i^t \parallel GID \parallel N_i^{t\prime} \parallel N_s^{t+1}\right)_{(C_i^t, R_i^t).}$ $MAC_2 = c(M_2 \parallel N_i^{t\prime} \parallel N_s^{t+1})$ M_2, MAC_2 ⟸	
	بازیابی $N_s^{t+1\prime}$ از M_2 $MAC_2' = C(M_2 \parallel N_i^t \parallel N_s^{t+1\prime})$ $MAC_2' =^? MAC_2$ $C_i^{i+1} = s\left(N_s^{t+1\prime} \parallel N_i^{t+1}\right)_{(C_i^t, R_i^t)}$ $R_i^{t+1} = P(C_i^{i+1})$ $M_3 = s\left(UID_i^t \parallel GID \parallel N_s^{t+1\prime} \parallel N_i^{t+1}\right)_{(C_i^t, R_i^t)}$ $M_4 = s\left(UID_i^t \parallel GID \parallel N_s^{t+1\prime} \parallel N_i^{t+1} \parallel R_i^{t+1}\right)_{(C_i^t, R_i^t)}$ $MAC_{34} = C(M_3 \parallel M_4 \parallel N_i^{t+1} \parallel R_i^{t+1})$ $sk_{i,s} = H(N_i^{t+1}) \oplus H(N_s^{t+1\prime})$ بروزرسانی $[ID_i, (C_i^t, R_i^t)]$ M_3, M_4, MAC_{34} ⟹
بازیابی $N_i^{t+1\prime}$ و N_i^t از M_3 $MAC'_{34} = C\left(M_3 \parallel M_4 \parallel N_i^{t+1\prime} \parallel R_i^{t+1\prime}\right)$ $=^? MAC_{34} MAC_{34}'$ $C_i^{i+1} = s(N_s^{t+1} \parallel N_i^{t+1\prime})_{(C_i^t, R_i^t)}$ $UID_i^{t+1\prime} = H(ID_i \parallel R_i^{t+1\prime})$ بروزرسانی $[ID_i, UID_i^{t+1\prime}, (C_i^{t+1}, R_i^{t+1\prime})]$ $sk_{s,i} = H(N_s^{t+1}) \oplus H(N_i^{t+1\prime})$	

شکل۵: فرآیند احراز هویت و توافق کلید نشست میان پهپاد و ایستگاه زمینی در پروتکل PMAP

۳. ارزیابی امنیتی پروتکل‌ها

در این بخش امنیت پروتکل‌هایی که در این مقاله توضیح داده شدند مورد مطالعه و بررسی قرار می‌گیرند. ارزیابی امنیت این پروتکل‌ها در دو بخش روش‌های غیرصوری و روش‌های صوری صورت می‌گیرد. برای ارزیابی امنیتی با روش‌های غیرصوری به نتایج ارائه شده توسط خود طراحان و مقالاتی که به این طرح‌ها حمله کردند، ارجاع می‌شود که به طور خلاصه مطابق جدول ۲ قابل بیان هستند.

جدول ۲: مقاومت سه پروتکل در برابر حملات شناخته شده

	مقاومت در برابر حمله							
پروتکل	شنود[1]	تکرار	تغییر پیام	ضبط پهپاد	مردی در میانه	جعل	همگام‌سازی[2]	محرمانگی روبه جلو[3]
SecAuthUAV	ندارد[۱۵]	دارد	ندارد[۴]	ندارد[۴]	دارد	دارد	دارد	دارد
Drone-MAP	دارد	دارد	ندارد[۴]	ندارد[۴]	ندارد[۱۴]	دارد	ندارد [۱۴]	ندارد[۱۵]
PMAP	ندارد[۱۵]	دارد	دارد	دارد	دارد	دارد	ندارد [۱۴]	ندارد[۱۵]

برای ارزیابی صوری این پروتکل‌ها در این مقاله روش تحلیل خودکار با استفاده از ابزار ProVerif به کار گرفته می‌شود که هر سه پروتکل با زبان ProVerif پیاده‌سازی شده و به صورت خودکار بررسی می‌شود که نشت اطلاعات دارند یا نه. لازم به ذکر است از آنجا که هسته اصلی امنیت در این پروتکل‌ها مربوط به بخش ارتباط پهپاد با ایستگاه زمینی است، در ارزیابی خودکار روی بخش مذکور تمرکز شده است و نشتی اطلاعات یا وجود ضعف در آن بررسی شده است. نتایج تحلیل این بخش قابل تعمیم به بخش‌های دیگر پروتکل‌ها مانند بخش احراز هویت پهپاد با پهپاد می‌باشد.

معرفی ابزار تحلیل خودکار ProVerif

ProVerif ابزاری برای تحلیل امنیتی خودکار پروتکل‌های رمزنگاری است که مبتنی بر روش‌های صوری طراحی شده است. این ابزار می‌تواند به صورت خودکار امکان نشت اطلاعات محرمانه در یک پروتکل را بررسی کند. همچنین با استفاده از ProVerif می‌توان بررسی کرد که احراز هویت میان نهادهای پروتکل به درستی انجام می‌شود یا نه. برای استفاده از ProVerif در ارزیابی صوری پروتکل‌ها، لازم است تا این پروتکل‌ها ابتدا با یک زبان قابل فهم برای این ابزار پیاده‌سازی شوند. بعد از این کار می‌بایست یک مهاجم همراه با توانمندی‌هایی که در اختیار دارد برای این ابزار مدل شود. حال پروتکل و مدل مهاجم در اختیار ابزار ProVerif گذاشته می‌شود و این ابزار به صورت خودکار و با روش‌های جستجو و بررسی کامپیوتری حالت‌های مختلف را که مهاجم می‌تواند از پروتکل بهره‌برداری غیر مجاز کند را کنترل می‌کند. اگر روزنه‌ها یا محاسباتی که باعث نشتی اطلاعات محرمانه شوند توسط این ابزار کشف شود، در خروجی خود اعلام می‌کند در غیر این صورت می‌گوید که پروتکل شرط لازم برای امنیت را دارد. بنابراین یک مرحله دیگر برای استفاده از ابزار خودکار ProVerif تجزیه و تحلیل نتایج خروجی آن هست [۱۲].

کدهای مربوط به پیاده‌سازی سه پروتکل SecAuthUAV، Drone-MAP و PMAP در پیوست الف این مقاله ارایه شده است. با اجرای این کدها در ابزار ProVerif خروجی‌های خلاصه شده در شکل‌های ۶، ۷ و ۸ حاصل می‌شود که به ترتیب مربوط به نتایج ارزیابی صوری پروتکل‌های SecAuthUAV، Drone-MAP و PMAP هستند. با توجه به این خروجی‌ها می‌توان نتیجه گرفت که هیچ کدام از این پروتکل‌ها نشت اطلاعات محرمانه ندارند و تمام آنها عمل احراز هویت بین پهپاد و ایستگاه زمینی را به صورت امن انجام می‌دهند. البته همان طور که گفته شد این تحلیل و ارزیابی نشان می‌دهد که شرط لازم (یا بهتر است گفته شود یکی از شرایط لازم) برای امنیت پروتکل‌ها برقرار است. شرط‌های لازم امنیت دیگر باید با کاربرد ابزارهای تحلیل خودکار، روش‌های صوری دیگر مانند روش‌های مبتنی بر منطق و روش‌های غیر صوری و حتی با استفاده از اثبات‌های ریاضیاتی بررسی شوند و در کنار هم یک برآورد از میزان امنیت پروتکل‌ها ارائه کنند.

[1] **Eavesdropping**
[2] **De-synchronization**
[3] **Forward secrecy**

```
Verification summary:
Query not attacker(R[]) is true.
Query not attacker(R'[]) is true.
Query not attacker(k1[]) is true.
Query not attacker(SKI[]) is true.
Query not attacker(k2[]) is true.
Query not attacker(X1[]) is true.
Query inj-event(A2) ==> inj-event(A1) is true.
Query inj-event(B2) ==> inj-event(B1) is true.
```

شکل ۶: نتایج تحلیل نشت اطلاعات محرمانه و احراز هویت امن پروتکل SecAuthUAV با ProVerif

```
Verification summary:
Query not attacker(km1[]) is true.
Query not attacker(R'[]) is true.
Query not attacker(km2[]) is true.
Query not attacker(km3[]) is true.
Query not attacker(km6[]) is true.
Query inj-event(A2) ==> inj-event(A1) is true.
Query inj-event(B2) ==> inj-event(B1) is true.
```

شکل ۷: نتایج تحلیل نشت اطلاعات محرمانه و احراز هویت امن پروتکل Drone-MAP با ProVerif

```
Verification summary:
Query not attacker(ri[]) is true.
Query not attacker(ri1[]) is true.
Query not attacker(ri1'[]) is true.
Query not attacker(ci1[]) is true.
Query not attacker(ski[]) is true.
Query not attacker(ci[]) is true.
Query inj-event(A2) ==> inj-event(A1) is true.
Query inj-event(B2) ==> inj-event(B1) is true.
Query inj-event(T2) ==> inj-event(T1) is true.
```

شکل ۸: نتایج تحلیل نشت اطلاعات محرمانه و احراز هویت امن پروتکل PMAP با ProVerif

۴. سرعت و کارآیی محاسباتی پروتکل‌های SecAuthUAV، Drone-MAP و PMAP

در کنار امنیت یک پروتکل رمزنگاری نباید از کارآیی آن در بسترهای سخت‌افزاری و نرم‌افزاری غافل ماند. به عبارت دیگر پروتکل مناسب برای کاربردهای خاص مانند شبکه پهپادها، پروتکلی است که علاوه بر امنیت لازم، از کارآیی مطلوبی برخوردار باشد. منظور از کارآیی یک الگوریتم یا پروتکل رمزنگاری، سرعت محاسباتی و عملکردی آن و نیازی که به منابع سخت‌افزاری یا نرم‌افزاری برای پیاده‌سازی لازم دارد، در نظر گرفته می‌شود.

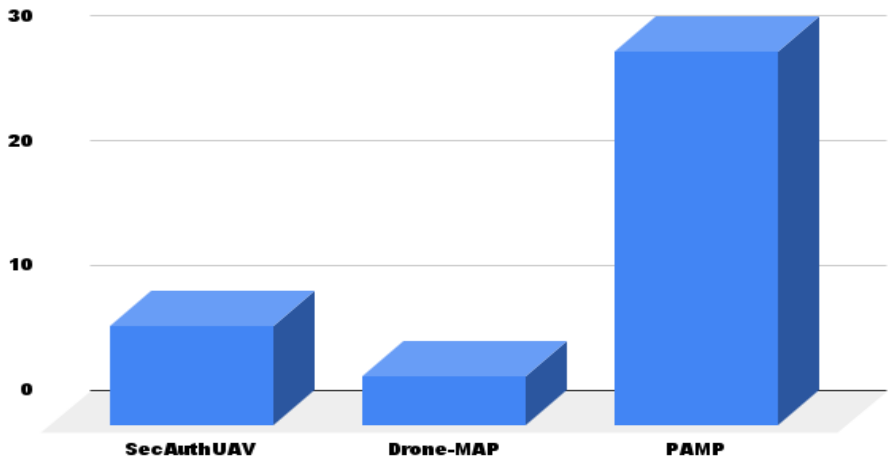
در این بخش سه پروتکل SecAuthUAV، Drone-MAP و PMAP که در بخش‌های قبل از لحاظ امنیتی مورد مطالعه قرار گرفتند از جهت سرعت و کارآیی محاسباتی با یکدیگر مقایسه می‌شوند. برای این کار از روش پیشنهادی در [۲۰] استفاده شده است که در آن زمان‌هایی برای سرعت محاسباتی عملگرهای مختلف در نظر گرفته شده و با شمارش تعداد این عملگرها در یک پروتکل، یک برآورد از سرعت محاسباتی پروتکل حساب می‌شود. به این ترتیب می‌توان سرعت محاسباتی پروتکل‌های مختلف که اصول طراحی یکسانی دارند را با یکدیگر مقایسه کرد. در [۲۰] زمان اجرای یک تابع چکیده ساز و کد احرازهویت پیام (HMAC) هرکدام ۴۶۰ نانوثانیه، زمان اجرای عملیات رمزنگاری و رمزگشایی (با یک الگوریتم رمز استاندارد) هرکدام ۸۰۰ نانوثانیه و زمان اجرای XOR و الحاق (در مقایسه با توابع چکیده‌ساز و رمزنگاری) تقریباً صفر در نظر گرفته شده است. با این حساب می‌توان زمان انجام عملیات رمزنگاری و رمزگشایی را تقریباً دو برابر زمان اجرای یک تابع چکیده‌ساز در نظر گرفت.

با بررسی پروتکل‌های بررسی شده در این مقاله مشاهده می‌شود که پروتکل SecAuthUAV محاسبات معادل ۸ تابع چکیده‌ساز، پروتکل Drone-MAP محاسبات معادل ۴ تابع چکیده‌ساز و پروتکل PMAP محاسبات معادل ۳۰ تابع چکیده‌ساز استفاده کرده‌اند که در پروتکل PMAP، هر تابع رمزنگاری با دو تابع چکیده‌ساز معادل شده است. بنابراین سرعت محاسباتی هر کدام از این طرح‌ها مطابق جدول ۳ قابل بیان هستند.

جدول ۳: مقایسه سرعت محاسباتی پروتکل‌های SecAuthUAV، Drone-MAP و PMAP

طرح‌ها	تابع چکیده‌ساز	رمزنگاری	xor	کداحرازهویت پیام(MAC)	الحاق	جمع(تابع چکیده ساز)	سرعت محاسباتی (نانوثانیه)
SecAuthUAV	۸	ندارد	۱۵	ندارد	۲۷	۸	۳۶۸۰
Drone-MAP	۴	ندارد	۱۶	ندارد	۲۱	۴	۱۸۴۰
PMAP	۶	۹	۲	۶	۳۶	۳۰	۱۳۸۰۰

اگر نتایج مقایسه سرعت محاسباتی پروتکل‌های SecAuthUAV، Drone-MAP و PMAP در قالب نمودار نشان داده شود، شکل ۹ حاصل می‌شود.



شکل ۹: سرعت محاسباتی سه پروتکل SecAuthUAV، Drone-MAP و PMAP

با توجه به نتایج مقایسه سرعت محاسباتی پروتکل‌ها مشاهده می‌شود که پروتکل PMAP به علت عملیات رمزنگاری که در محاسبات خود استفاده می‌کند در مقایسه با دو پروتکل دیگر که از تابع چکیده‌ساز استفاده کرده‌اند، نیاز به زمان بیشتری برای احراز هویت نهادهای خود دارد. همچنین با توجه به این مقایسه‌ها می‌توان نتیجه گرفت که از میان سه پروتکل، پروتکل Drone-MAP سرعت محاسباتی بالاتری دارد.

۵. نتیجه‌گیری

پروتکل‌های امنیتی نقش مهم و انکارناپذیری در تامین امنیت کاربردهای مختلف مانند استفاده از شبکه پهپادها دارند. برای اطمینان از کاربرد صحیح یک پروتکل امنیتی لازم است تا این پروتکل‌ها با استفاده از روش‌های صوری و غیرصوری مورد تحلیل و ارزیابی قرار گیرند. به طوری که تنها تحلیل با استفاده از یک روش (چه صوری و چه غیرصوری) نمی‌تواند اطمینان خاطر خوبی از امنیت پروتکل‌ها ایجاد کند و لازم است تا هر دو روش کنار هم استفاده شوند. در میان روش‌های صوری نیز، روش‌های تحلیل خودکار از دقت و سرعت بالایی برخوردار هستند. علاوه بر بحث امنیت یک پروتکل امنیتی لازم است تا پروتکل از کارآیی مطلوبی نیز برخوردار باشد که منظور از آن سرعت محاسباتی مطلوب و نیاز به منابع مناسب برای پیاده‌سازی نرم‌افزاری یا سخت‌افزاری هست.

در این مقاله روی پروتکل‌های احراز هویت مناسب برای شبکه پهپادها که مبتنی بر توابع کپی‌ناپذیر فیزیکی طراحی شده بودند، تمرکز شد و سه پروتکل SecAuthUAV، Drone-MAP و PMAP مورد مطالعه و بررسی قرار گرفتند. اگر چه این پروتکل‌ها با روش‌های غیر صوری و روش مبتنی بر منطق مورد ارزیابی امنیتی قرار گرفته بودند اما در تحلیل آنها (به جز PMAP که برای تحلیل خودکار آن از ابزار Avispa استفاده شده است) از ابزارهای تحلیل خودکار استفاده نشده بود. بنابراین از یک ابزار تحلیل خودکار به نام ProVerif استفاده شد تا پروتکل‌های SecAuthUAV، Drone-MAP و PMAP از نظر تحلیل صوری با ابزارهای خودکار نیز مورد بررسی قرار بگیرند. نتایج تحلیل برای هر سه پروتکل نشان می‌دهد که آنها شرط لازم امنیتی از نگاه ابزارهای تحلیل خودکار را دارند که باعث افزایش اطمینان در کنار نتایج سایر تحلیل‌ها خواهد بود. در انتهای این مقاله سه پروتکل ذکر شده از لحاظ سرعت محاسباتی با یکدیگر مقایسه شدند که پروتکل PMAP به دلیل استفاده از عملیات رمزنگاری در مقایسه با دو پروتکل دیگر که تنها از توابع چکیده‌ساز پیام استفاده کرده بودند، کندتر هست و پروتکل Drone-MAP نسبت به دو پروتکل دیگر سرعت بالاتری دارد. بنابراین از دید تحلیل صوری با ابزارهای تحلیل خودکار، پروتکل پروتکل Drone-MAP در مقایسه با دو پروتکل دیگر یک پروتکل مناسب‌تر جهت کاربرد در شبکه پهپادها خواهد بود.

منابع

[۱] Y. Zhi, Z. Fu, X. Sun, and J. Yu, "Security and privacy issues of UAV: a survey," *Mobile Networks and Applications*, vol. 25, no. 1, pp. 95-101, 2020.

[۲] L. Gupta, R. Jain, and G. Vaszkun, "Survey of important issues in UAV communication networks," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 2, pp. 1123-1152, 2015.

[۳] A. Yazdinejad, R. M. Parizi, A. Dehghantanha, H. Karimipour, G. Srivastava, and M. Aledhari, "Enabling drones in the internet of things with decentralized blockchain-based security," *IEEE Internet of Things Journal*, vol. 8, no. 8, pp. 6406-6415, 2020.

[۴] C. Pu, A. Wall, K.-K. R. Choo, I. Ahmed, and S. Lim, "A Lightweight and Privacy-Preserving Mutual Authentication and Key Agreement Protocol for Internet of Drones Environment ",*IEEE Internet of Things Journal*, 2022.

[۵] L. Liu and J. Cao, "Analysis of One Lightweight Authentication and Key Agreement Scheme for Internet of Drones," *Computer Communications*, vol. 154, pp. 455-464, 2020.

[۶] S. Chen, S. Cui, and J. Liu, "A Lightweight Authentication Protocol for 5G Cellular Network Connected Drones," in *International Conference on Heterogeneous Networking for Quality, Reliability, Security and Robustness*, 2021, pp. 129-143: Springer.

[۷] C.-M. Chen and S. Liu, "Improved secure and lightweight authentication scheme for next-generation IOT infrastructure," *Security and Communication Networks*, vol. 2021, 2021.

[۸] G.-h. Wei, Y.-l. Qin, and W. Fu, "An Improved Security Authentication Protocol for Lightweight RFID Based on ECC," *Journal of Sensors*, vol. 2022, 2022.

[۹] J. Alizadeh, M. Safkhani, and A. Allahdadi, "ISAKA: Improved Secure Authentication and Key Agreement protocol for WBAN," *Wireless Personal Communications*, pp. 1-25, 2022.

[۱۰] B. A. Alzahrani, A. Irshad, A. Albeshri, K .Alsubhi, and M. Shafiq, "An improved lightweight authentication protocol for wireless body area networks," *IEEE Access*, vol. 8, pp. 190855-190872, 2020.

[۱۱] L. Vigano, "Automated security protocol analysis with the AVISPA tool," *Electronic Notes in Theoretical Computer Science*, vol. 155, pp. 61-86, 2006.

[۱۲] B. Blanchet, B. Smyth, V. Cheval, and M. Sylvestre, "Proverif 2.00: automatic cryptographic protocol verifier, user manual and tutoria," ed: Jul, 2020.

[۱۳] C. J. Cremers, "The Scyther Tool: Verification, falsification, and analysis of security protocols," in *International conference on computer aided verification*, 2008, pp. 414-418: Springer.

[۱۴] T. Alladi, G. Bansal, V. Chamola, and M. Guizani, "SecAuthUAV: A novel authentication scheme for UAV-ground station and UAV-UAV communication," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 12, pp. 15068-15077, 2020.

[۱۵] T. Alladi, V. Venkatesh, V. Chamola, and N. Chaturvedi, "Drone-MAP: A novel authentication scheme for drone-assisted 5G networks," in *IEEE INFOCOM 2021-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, 2021, pp. 1-6: IEEE.

[۱۶] G. Bansal, N. Naren, V. Chamola, B. Sikdar, N. Kumar, and M. Guizani, "Lightweight mutual authentication protocol for V2G using physical unclonable function," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 7, pp. 7234-7246, 2020.

[۱۷] B. Chatterjee, D. Das, S. Maity, and S. Sen, "RF-PUF: Enhancing IoT security through authentication of wireless nodes using in-situ machine learning," *IEEE Internet of Things Journal*, vol. 6, no. 1, pp. 388-398, 2018.

[۱۸] T. Alladi, V. Chamola, and N. Kumar, "PARTH: A two-stage lightweight mutual authentication protocol for UAV surveillance networks," *Computer Communications*, vol. 160, pp. 81.۲۰۲۰ ,۹۰-

[۱۹] T. Nie, C. Song, and X. Zhi, "Performance evaluation of DES and Blowfish algorithms," in *2010 International conference on biomedical engineering and computer science*, 2010, pp. 1-4: IEEE.

[۲۰] **A. Kabra, S. Kumar, and G. S. Kasbekar, "Efficient, flexible and secure group key management protocol for dynamic iot settings,"** ***arXiv preprint arXiv:2008.06890,*** **2020.**

پیوست الف

در این پیوست کدهای ProVerif تهیه شده برای پروتکل‌های SecAuthUAV، Drone-MAP و PMAP ارایه شده است.

```
free C1: channel.
free R: bitstring[private].
free R': bitstring[private].
free H1: bitstring.
free H1': bitstring.
free H2: bitstring.
free H2': bitstring.
free H3: bitstring.
free H3': bitstring.
free k1: bitstring[private].
free k2: bitstring[private].
free N': bitstring.
free GID: bitstring.
free TUIDI: bitstring.
free X1: bitstring[private].
free Y2: bitstring.
free Q: bitstring.
free M': bitstring.
free w: bitstring.
free w1: bitstring.
free na: bitstring.
free SKI: bitstring[private].
free SKI': bitstring[private].
(*.....*)
fun xor(bitstring, bitstring): bitst
equation forall p: bitstring, u: bits
xor(xor(p, u), u) = p.
fun concat(bitstring, bitstring): bitstr
fun h(bitstring): bitstring.
(*.....
*)
query attacker(R).
query attacker(R').
query attacker(k1).
event A1.
event A2.
event B1.
event B2.
(*.....*)
let ui =
new na: bitstring;
let H1
= h(concat(R, concat(TUIDI, na))) in
event A1;
out(C1, (TUIDI, na, H1));
in(C1, y: bitstring);
let w = concat(Y2, X1) in
let w1 = xor(concat(k1, k2), Q) in
let nb = xor(Y2
X1, k1)) in
let na = xor(X1, k2) in
let H2'
= h(concat(Q, concat(GID, concat(na, n
if H2 = H2' then
event B2;
new nc: bitstring;
let M' = xor(R', concat(k1, k2)) in
let N' = xor(nc, k1) in
let SKI = concat(xor(k1, nb), xor(k2, nc)) in
let H3
= h(concat(R', concat(TUIDI, concat(nb, concat(nc,
out(C1, (M', N', H3));
0.
(*.....*)
let GS =
in(C1, x: bitstring);
let H1' = h(concat(R, concat(TUIDI, na))) in
if H1 = H1' then
event A2;
new nb: bitstring;
let X1 = xor(na, k2) in
let Y2 = xor(nb, (X1, k1)) in
let Q = xor(concat(Y2, X1), concat(k2, k1)) in
let H2
= h(concat(Q, concat(GID, concat(na, nb)))) in
event B1;
out(C1, (Q, H2));
in(C1, z: bitstring);
```

شکل الف -۱: کدهای پروتکل SecAuthUAV در ProVerif

```
free C1: channel.
free R: bitstring[private].
free R': bitstring[private].
free c': bitstring[private].
free km2: bitstring[private
free km3: bitstring[private
free km4: bitstring[private
free km5: bitstring[private
free km6: bitstring[private
free km1: bitstring[private
free km: bitstring[private].
free km1': bitstring[private
free H1: bitstring.
free H1': bitstring.
free H2: bitstring.
free H2': bitstring.
free H3: bitstring.
free H3': bitstring.
free N: bitstring.
free N': bitstring.
free GID: bitstring.
free TUIDI: bitstring.
free Xm1: bitstring.
free Ym: bitstring.
free Q: bitstring.
free M': bitstring.
free w: bitstring.
free m'': bitstring.
free c: bitstring.
free w1: bitstring.
free m1: bitstring.
free na: bitstring.
free nb: bitstring.
(*.....*)
fun xor(bitstring, bitstring): bitst
ring.
equation forall p: bitstring, u: bitstring
xor(xor(p, u), u) = p.
fun concat(bitstring, bitstring): bitstri
fun h(bitstring): bitstring.
(*.....*)
query attacker(km1).
query attacker(R').
query attacker(km2).
query attacker(km3).
query attacker(km6).
query inj − event(A2) ==
> inj
− event(A1).
query inj − event(B2) ==
> inj
− event(B1).
(*.....*)
event A1.
event A2.
event B1.
event B2.
(*.....*)
let ui =
new na: bitstring;
out(C1, (TUIDI, na));
in(C1, y: bitstring);
let m1 = xor(N, km1) in
let w = concat(Ym, Xm1) in
let w1 = xor(concat(km, km1'), Q) in
new nc: bitstring;
event B2;
let m'' = xor(c', km2) in
let M' = xor(R', km3) in
let N' = xor(nc, km4) in
let SKI = xor(xor(km5, nb), xor(km6, nc)) in
event A2;
let H3
= h(concat(R', concat(TUIDI, concat(m1, concat(nc, SKI))
out(C1, (M', N', m'', H3));
0.
(*.....*)
let GS =
in(C1, x: bitstring);
new nb: bitstring;
let Q = xor(concat(Ym, Xm1), concat(km, km1')) in
let N = xor(m1, km1) in
let H2
= h(concat(Q, concat(GID, concat(na, concat(m1, nb))))) i
event B1;
out(C1, (Q, c, N, H2));
in(C1, z: bitstring);
let c' = xor(m'', km2) in
let R' = xor(M', km3) in
let nc = xor(N', km4) in
let SKI' = xor(xor(km5, nb), xor(km6, nc)) in
if SKI = SKI' then
event A1;
let H3'
= h(concat(R', concat(TUIDI, concat(m1, concat(nc, SKI))
if H3' = H3 then
0.
process
ui|GS
```

```
free SKI: bitstring[private]   let
free SKI': bitstring[private
```

شکل الف – ۲: کدهای پروتکل Drone-MAP در ProVerif

```
free c1: channel.
free ri: bitstring[private].
free ski: bitstring[private].
free pid: bitstring.
free idi: bitstring.
free ci: bitstring[private].
free m1: bitstring.
free m2: bitstring.
free m3: bitstring.
free m4: bitstring.
free m1': bitstring.
free m2': bitstring.
free m3': bitstring.
free m4': bitstring.
free zs: bitstring.
free mac1: bitstring.
free mac1': bitstring.
free mac2: bitstring.
free mac2': bitstring.
free mac34: bitstring.
free mac34': bitstring.
free ns: bitstring[private].
free ni: bitstring[private].
free ni1: bitstring[private].
free ci1: bitstring[private].
free f: bitstring.
free ri1: bitstring[private].
free ri1': bitstring[private].
(*.....
(* functions *)
type key.
fun senc(bitstring, key): bitstr
reduc forall m: bitstring, K: ke
sdec(senc(m, K), K) = m.
fun xor(bitstring, bitstring): b
equation forall p: bitstring, q:
```

```
xor(xor(p, q), q) = p.
fun concat(bitstring, bitstring): bitstring.
fun h(bitstring): bitstring.
type mkey.
fun mac(bitstring, mkey): bitstring.
reduc forall m: bitstring, k: mkey; get_mess
= m.
(*.....*)
query attacker(ri).
query attacker(ri1).
query attacker(ri1').
query attacker(ci1).
query attacker(ski).
query attacker(ci).
query inj − event(A2) ==
                > inj − event(A1).
query inj − event(B2) ==
                > inj − event(B1).
query inj − event(T2) ==
                > inj − event(T1).

(*.....*)
process *)
let uav(k1: key, k: mkey) =
let pid = h(concat(idi, ri)) in
new ni: bitstring;
let m1 = senc(concat(pid, concat(zs, ni)),
k1) in
let mac1 = mac(concat(m1, ni), k) in
event T1;
out(c1, (m1, mac1));
in(c1, x: bitstring);
let m2' = sdec(m2, k1) in
let mac2'
= mac(concat(m1, concat(ni, ns)), k) in
if mac2 = mac2' then
event A1;
new ni1: bitstring;
```

```
let ci1 = senc(concat(ns, ni1), k1) in
let m3
= senc(concat(pid, concat(zs, concat(ni1, ns))), k
let m4
= senc(concat(pid, concat(zs, concat(ni1, concat(
let mac34
= mac(concat(m3, concat(m4, concat(ni, ri1))), k
event B2;
let ski = xor(h(ni1), h(ns)) in
out(c1, (m3, m4, mac34));
0.
let gs(k1: key, k: mkey) =
let pid' = sdec(pid, k1) in
let f = get_message(mac1) in
let mac1' = mac(concat(m1, ni), k) in
if mac1 = mac1' then
event T1;
new ns: bitstring;
let m2
= senc(concat(pid, concat(zs, concat(ni, ns))), k1
let mac2
= mac(concat(m1, concat(ni, ns)), k) in
event A2;
out(c1, (m2, mac2));
in(c1, (y: bitstring));
let m3' = sdec(m3, k1) in
let m4' = sdec(m4, k1) in
let mac34'
= mac(concat(m3, concat(m4, concat(ni, ri1))), k
if mac34 = mac34' then
event B1;
let pid' = h(concat(idi, ri1')) in
let ski = xor(h(ni1), h(ns)) in
0.
(*.....*)
process
new k: mkey;
new k1: key;
!uav(k1, k)|!gs(k1, k)
```

شکل الف – ۳: کدهای پروتکل **PMAP** در ProVerif